Cheating Prevention in Secret Sharing over $GF(p^t)$

Josef Pieprzyk[1] and Xian-Mo Zhang[2]

[1] Department of Computing, Macquarie University
Sydney , NSW 2109, AUSTRALIA
josef@ics.mq.edu.au
[2] School of IT and CS, University of Wollongong
Wollongong NSW 2522, AUSTRALIA
xianmo@cs.uow.edu.au

Abstract. The work investigates cheating prevention in secret sharing. It is argued that cheating is immune against cheating if the cheaters gain no advantage over honest participants by submitting invalid shares to the combiner. This work addresses the case when shares and the secret are taken from $GF(p^t)$. Two models are considered. The first one examines the case when cheaters consistently submit always invalid shares. The second model deals with cheaters who submit a mixture of valid and invalid shares. For these two models, cheating immunity is defined, properties of cheating immune secret sharing are investigated and their constructions are given.

Keywords: Secret Sharing, Nonlinear Secret Sharing, Cheating Immunity

1 Introduction

Secret sharing is widely used to produce group-oriented cryptographic algorithms, systems and protocols. Tompa and Woll [11] showed that Shamir secret sharing can be subject to cheating by dishonest participants. It is easy to see that, in fact, dishonest participants can cheat in any linear secret sharing. Cheating prevention has been addressed in literature for conditionally and unconditionally secure secret sharing. For conditionally secure secret sharing, the combiner checks validity of submitted shares before attempting to compute the secret. Any invalid share (and the cheater) is likely to be detected before the secret reconstruction (see [2, 1, 6]). Publicly verifiable secret sharing (see [3, 5, 9, 7]) provide a solution to this problem in the conditionally secure setting. We argue that instead of setting an expensive verification infrastructure to detect cheaters, it is possible to discourage them from cheating. It is likely that cheaters will be discouraged if they are not able to reconstruct the valid secret from the invalid one returned by the combiner. Ideally, submission of invalid shares should not give any advantage to the cheaters over the honest participants in recovery of the valid secret. In this work shares and the secret are from $GF(p^t)$. The structure of the paper is as follows. First we introduce a basic model of cheating in which, cheaters always submit invalid shares. Cheating immunity is defined and constructions of cheating immune secret sharing are given. Further we generalise our model for the case where the collaborating cheaters may submit an arbitrary mixture of their valid and invalid shares. Again, the notion of strict immunity is introduced, its properties are investigated and constructions are shown.

2 Basic Model of Cheating

Let $GF(p^t)$ denote a finite field with p^t elements where p is a prime number and t in a positive integer. We write $GF(p^t)^n$ to denote the vector space of n tuples of elements from $GF(p^t)$. Then each vector $\alpha \in GF(p^t)^n$ can be expressed as $\alpha = (a_1, \ldots, a_n)$ where $a_1, \ldots, a_n \in GF(p^t)$. We consider a mapping f from $GF(p^t)^n$ to $GF(p^t)$. Usually we write f as $f(x)$ or $f(x_1, \ldots, x_n)$ where $x = (x_1, \ldots, x_n)$ and each $x_j \in GF(p^t)$. f is also called a *function* on $GF(p^t)^n$. f is said to be *balanced* if $f(x)$ takes each element of $GF(p^t)$ precisely $p^{t(n-1)}$ times while x goes through each vector in $GF(p^t)^n$ once. The *Hamming weight* of a vector $\alpha \in GF(p^t)^n$, denoted by $HW(\alpha)$, is the number of nonzero coordinates of α. An *affine* function f on $GF(p^t)^n$ is a function that takes the form of $f(x_1, \ldots, x_n) = a_1x_1 + \cdots + a_nx_n + c$, where $+$ denotes the addition in $GF(p^t)$, $a_j, c \in GF(p^t)$, $j = 1, 2, \ldots, n$. Furthermore f is called a *linear* function if $c = 0$. It is easy to verify that any non-constant affine function is balanced.

We see secret sharing as a set of distribution rules combined into a single table $\mathcal{T}$ (see [10]) with entries from $GF(p^t)$. We also assume that we are dealing with (n, n) threshold scheme where any n participants are able to determine a single entry from $\mathcal{T}$ which indicates the secret. Our considerations are restricted to the case of (n, n) secret sharing. The general case of (n, N) secret sharing can be seen as a concatenation of (n, n) secret sharing with a system of N "consistent" linear equations. Shares are generated for N participants using the linear equations. Any n participants can get a system of linear equations with a unique solution which points out the unique row of the table $\mathcal{T}$. Let $x = (x_1, \ldots, x_n)$ and $\delta = (\delta_1, \ldots, \delta_n)$ be two vectors in $GF(p^t)^n$. Define a vector $x_\delta^+ \in GF(p^t)^n$, whose j-th coordinate is x_j if $\delta_j \neq 0$, or 0 if $\delta_j = 0$. In addition, we define a vector $x_\delta^- \in GF(p^t)^n$, whose j-th coordinate is 0 if $\delta_j \neq 0$, or x_j if $\delta_j = 0$. Let $\tau = (\tau_1, \ldots, \tau_n)$ and $\delta = (\delta_1, \ldots, \delta_n)$ be two vectors in $GF(p^t)^n$. We write $\tau \preceq \delta$ to denote the property that if $\tau_j \neq 0$ then $\delta_j \neq 0$. In addition, we write $\tau \prec \delta$ to denote the property that $\tau \preceq \delta$ and $HW(\tau) < HW(\delta)$. In particular, if $\delta' \preceq \delta$ and $HW(\delta') = HW(\delta)$ we write $\delta \bowtie \delta'$. It is easy to verify that $\delta \bowtie \delta' \iff \delta' \preceq \delta$ and $\delta \preceq \delta' \iff$ both $x_\delta^+ = x_{\delta'}^+$ and $x_\delta^- = x_{\delta'}^-$ hold for any $x \in GF(p^t)^n$, where $\iff$ denotes "if and only if". We define the following notation that will be frequently used in this paper. Let δ be a nonzero vector in $GF(p^t)^n$, $\tau \preceq \delta$ and $u \in GF(p^t)$. Set

$$R_f(\delta, \tau, u) = \{x_\delta^- | f(x_\delta^- + \tau) = u\} \tag{1}$$

We also simply write $R_f(\delta, \tau, u)$ as $R(\delta, \tau, u)$ if no confusions occur.

Lemma 1. *Let δ be a nonzero vector in $GF(p^t)^n$, $\tau \preceq \delta$, and $u \in GF(p^t)$. Then for any given function f on $GF(p^t)^n$, (i) $R(\delta, \tau, u) = R(\delta', \tau, u)$ if $\delta' \bowtie \delta$, (ii) $R(\delta, \alpha_\delta^+, u) = R(\delta, \gamma_\delta^+, u)$ for any $\alpha, \gamma \in GF(p^t)^n$ with $\alpha_\delta^+ = \gamma_\delta^+$, (iii) there exists some $b \in GF(p^t)$ such that $R(\delta, \tau, b) \neq \emptyset$, where $\emptyset$ denotes the empty set.*

Proof. As (i) and (ii) hold obviously, we only prove (iii). Let γ be any vector in $GF(p^t)^n$. Set $f(\gamma_\delta^- + \tau) = b$. By definition, $\gamma_\delta^- \in R_f(\delta, \tau, b)$ and thus $R(\delta, \tau, b) \neq \emptyset$. $\square$

Given a function f on $GF(p^t)^n$, we introduce the following notations:

- Let $\alpha \in GF(p^t)^n$ be the sequence of shares held by the group $\mathcal{P} = \{P_1, \ldots, P_n\}$ of n participants and the secret $K = f(\alpha)$.
- The collection of cheaters is determined by the sequence $\delta = (\delta_1, \delta_2, \ldots, \delta_n)$ where P_i is a cheater $\Longleftrightarrow \delta_i$ is nonzero.
- At the pooling time, the cheaters submit their shares. It is assumed that cheaters always submit invalid shares. The honest participants always submit their valid shares. We consider the vector $\alpha + \delta$. From the properties of x_δ^+ and x_δ^-, $\alpha + \delta = \alpha_\delta^- + \alpha_\delta^+ + \delta$. Thus the combiner obtains $\alpha + \delta$ that splits into two parts: α_δ^- – the part submitted by honest participants, and $\alpha_\delta^+ + \delta$ – the part submitted by cheaters. The combiner returns an invalid secret $K^* = f(\alpha + \delta)$. Note that the cheaters always change their shares. We assume that there exists at least one cheater, in other words, δ is nonzero or $HW(\delta) > 0$.
- α_δ^+ determines valid shares held by the cheaters. The set $R(\delta, \alpha_\delta^+, K)$, or $\{x_\delta^- | f(x_\delta^- + \alpha_\delta^+) = K\}$, determines a collection of rows of $\mathcal{T}$ with the correct secret K and valid shares held by the cheaters.
- The set $R(\delta, \alpha_\delta^+ + \delta, K^*)$, or $\{x_\delta^- | f(x_\delta^- + \alpha_\delta^+ + \delta) = K^*\}$, represents the view of the cheaters after getting back K^* from the combiner.

The function f is called the *defining function* as it determines the secret sharing. The nonzero vector $\delta = (\delta_1, \ldots, \delta_n)$ is called a *cheating vector*, α is called a *original vector*. The value of $\rho_{\delta,\alpha} = \#(R(\delta, \alpha_\delta^+ + \delta, K^*) \cap R(\delta, \alpha_\delta^+, K))/\#R(\delta, \alpha_\delta^+ + \delta, K^*)$, expresses the probability of cheater success with respect to δ and α, where $\#X$ denotes the number of elements in the set X. As an original vector α is always in $R(\delta,\ \alpha_\delta^+ + \delta,\ K^*) \cap R(\delta,\ \alpha_\delta^+, K)$, the probability of successful cheating always satisfies $\rho_{\delta,\alpha} > 0$. Clearly the number of cheaters is equal to $HW(\delta)$.

Theorem 1. *Given a secret sharing scheme with its defining function f on $GF(p^t)^n$. Let $\delta \in GF(p^t)^n$ with $0 < HW(\delta) < n$ be a cheating vector and α be an original vector in $GF(p^t)^n$. If $\rho_{\delta,\alpha} < p^{-t}$ then there exists a vector $\gamma \in GF(p^t)^n$ such that $\rho_{\delta,\gamma} > p^{-t}$.*

Proof. Let $f(\alpha) = K$ and $f(\alpha + \delta) = K^*$. By definition, $R(\delta, \alpha_\delta^+, K) = \{x_\delta^- | f(x_\delta^- + \alpha_\delta^+) = K\}$ and $R(\delta, \alpha_\delta^+ + \delta, K^*) = \{x_\delta^- | f(x_\delta^- + \alpha_\delta^+ + \delta) = K^*\}$. We partition $R(\delta, \alpha_\delta^+ + \delta, K^*)$ into p^t parts: $R(\delta, \alpha_\delta^+ + \delta, K^*) = \cup_{u \in GF(p^t)} Q_u$ where $Q_u = R(\delta, \alpha_\delta^+ + \delta, K^*) \cap R(\delta, \alpha_\delta^+, u + K)$. Clearly $\#R(\delta, \alpha_\delta^+ + \delta, K^*) = \sum_{u \in GF(p^t)} \#Q_u$. Note that $R(\delta, \alpha_\delta^+ + \delta, K^*) \cap R(\delta, \alpha_\delta^+, K) = Q_0$. Therefore $\rho_{\delta,\alpha} = \#(R(\delta, \alpha_\delta^+ + \delta, K^*) \cap R(\delta, \alpha_\delta^+, K))/\#R(\delta, \alpha_\delta^+ + \delta, K^*) = \#Q_0/\#R(\delta, \alpha_\delta^+ + \delta, K^*)$. Since $\rho_{\delta,\alpha} < p^{-t}$, we have $\#Q_0/\#R(\delta, \alpha_\delta^+ + \delta, K^*) < p^{-t}$. It follows that $\#Q_0 < p^{-t}\#R(\delta, \alpha_\delta^+ + \delta, K^*)$. Thus we know that $\sum_{u \in GF(p^t), u \neq 0} \#Q_u > (1 - p^{-t})\#R(\delta, \alpha_\delta^+ + \delta, K^*)$. Thus there exists some $b \in GF(p^t)$ with $b \neq 0$ such that $\#Q_b > p^{-t}\#R(\delta, \alpha_\delta^+ +$

$\delta, K^*)$. By definition, $Q_b = \{x_\delta^- | f(x_\delta^- + \alpha_\delta^+ + \delta) = K^*,\ \ f(x_\delta^- + \alpha_\delta^+) = b + K\}$. Then there exists a vector $\beta_\delta^- \in Q_b$ and then $f(\beta_\delta^- + \alpha_\delta^+ + \delta) = K^*$, $f(\beta_\delta^- + \alpha_\delta^+) = b + K$. Set $\gamma = \beta_\delta^- + \alpha_\delta^+$. Thus $f(\gamma + \delta) = K^*$ and $f(\gamma) = b + K$. Clearly $\gamma_\delta^+ = \alpha_\delta^+$ and $\gamma_\delta^- = \beta_\delta^-$. Next we choose γ as an original vector. Due to $R(\delta, \gamma_\delta^+ + \delta,\ K^*) = \{x_\delta^-\ | f(x_\delta^- + \gamma_\delta^+ + \delta) = K^*\}$, $R(\delta, \gamma_\delta^+, b + K) = \{x_\delta^- | f(x_\delta^- + \gamma_\delta^+) = b + K\}$ and $\gamma_\delta^+ = \alpha_\delta^+$, we know that $R(\delta, \gamma_\delta^+ + \delta, K^*) \cap R(\delta, \gamma_\delta^+, b + K) = Q_b$ and $\rho_{\delta,\gamma} = \#(R(\delta, \gamma_\delta^+ + \delta, K^*) \cap R(\delta, \gamma_\delta^+, b+K))/\#R(\delta, \gamma_\delta^+ + \delta, K^*) = \#Q_b/\#R(\delta, \gamma_\delta^+ + \delta, K^*) = \#Q_b/\#R(\delta, \alpha_\delta^+ + \delta, K^*) > p^{-t}$. □

2.1 *k*-Cheating Immune Secret Sharing Scheme

Given a secret sharing with its defining function f on $GF(p^t)^n$. For a fixed nonzero $\delta \in GF(p^t)^n$, due to Theorem 1, $\min\{\rho_{\delta,\alpha} | \alpha \in GF(p^t)^n\} < p^{-t}$ implies that $\max\{\rho_{\delta,\alpha} | \alpha \in GF(p^t)^n\} > p^{-t}$. Therefore it is desirable that $\rho_{\delta,\alpha} = p^{-t}$ holds for every $\alpha \in GF(p^t)^n$. A secret sharing is said to be *k-cheating* if $\rho_{\delta,\alpha} = p^{-t}$ holds for every $\delta \in GF(p^t)^n$ with $1 \leq HW(\delta) \leq k$ and every $\alpha \in GF(p^t)^n$.

Theorem 2. *Given a secret sharing with its defining function f on $GF(p^t)^n$. Then this secret sharing is k-cheating immune $\Longleftrightarrow$ for any integer l with $1 \leq l \leq k$, any $\delta \in GF(p^t)^n$ with $HW(\delta) = l$, any $\tau \preceq \delta$ and any $u, v \in GF(p^t)$, the following conditions hold simultaneously: (i) $\#R(\delta, \tau, v) = p^{t(n-l-1)}$, (ii) $\#(R(\delta, \tau, v) \cap R(\delta, \tau + \delta, u)) = p^{t(n-l-2)}$.*

Proof. Assume that the secret sharing is k-cheating immune. Choose δ as a cheating vector and any vector $\alpha \in GF(p^t)^n$ as an original vector. Due to Lemma 1, there exist $a, b \in GF(p^t)$ such that $R(\delta, \alpha_\delta^+ + \delta, a) \neq \emptyset$ and $R(\delta, \alpha_\delta^+, b) \neq \emptyset$. Note that $R(\delta, \alpha_\delta^+ + \delta, a)$ can be partitioned into p^t parts: $R(\delta, \alpha_\delta^+ + \delta, a) = \bigcup_{v \in GF(p^t)} R(\delta, \alpha_\delta^+ + \delta, a) \cap R(\delta, \alpha_\delta^+, v)$. Assume that $R(\delta, \alpha_\delta^+ + \delta, a) \cap R(\delta, \alpha_\delta^+, v) \neq \emptyset$ for some $v \in GF(p^t)$. Then there exists a vector $\beta_\delta^- \in R(\delta, \alpha_\delta^+ + \delta, a) \cap R(\delta, \alpha_\delta^+, v)$. Set $\gamma = \beta_\delta^- + \alpha_\delta^+$. Since the secret sharing is k-cheating immune, $\#(R(\delta, \gamma_\delta^+ + \delta, a) \cap R(\delta, \gamma_\delta^+, v))/\#R(\delta, \gamma_\delta^+ + \delta, a) = \rho_{\delta,\gamma} = p^{-t}$, where $\gamma_\delta^+ = \alpha_\delta^+$. Thus $\#R(\delta, \alpha_\delta^+ + \delta, a) = p^t \#(R(\delta, \alpha_\delta^+ + \delta, a) \cap R(\delta, \alpha_\delta^+, v))$ whenever $R(\delta, \alpha_\delta^+ + \delta, a) \cap R(\delta, \alpha_\delta^+, v) \neq \emptyset$. It follows that $\#R(\delta, \alpha_\delta^+ + \delta, a) = \sum_{v \in GF(p^t)} \#(R(\delta, \alpha_\delta^+ + \delta, a) \cap R(\delta, \alpha_\delta^+, v))$. Combing the above two equalities, we know that $R(\delta, \alpha_\delta^+ + \delta, a) \cap R(\delta, \alpha_\delta^+, v) \neq \emptyset$ for every $v \in GF(p^t)$ and thus $\#(R(\delta, \alpha_\delta^+ + \delta, a) \cap R(\delta, \alpha_\delta^+, v)) = p^{-t} \#R(\delta, \alpha_\delta^+ + \delta, a)$ for every $v \in GF(p^t)$. Replacing α, δ, by $\alpha + \delta$, $(p-1)\delta$ respectively, due to the same arguments, we have $\#(R((p-1)\delta, \alpha_\delta^+ + p\delta, b) \cap R((p-1)\delta, \alpha_\delta^+ + \delta, u)) = p^{-t} \#R((p-1)\delta, \alpha_\delta^+ + p\delta, b)$ for every $u \in GF(p^t)$. Since the characteristic of the finite field $GF(p^t)$ is p, $pe = 0$ for every $e \in GF(p^t)$. It follows that $\#(R((p-1)\delta, \alpha_\delta^+, b) \cap R((p-1)\delta, \alpha_\delta^+ + \delta, u)) = p^{-t} \#R((p-1)\delta, \alpha_\delta^+, b)$ for every $u \in GF(p^t)$. Using Lemma 1, we obtain $\#(R(\delta, \alpha_\delta^+, b) \cap R(\delta, \alpha_\delta^+ + \delta, u)) = p^{-t} \#R(\delta, \alpha_\delta^+, b)$ for every $u \in GF(p^t)$. Recall that $R(\delta, \alpha_\delta^+ + \delta, a) \neq \emptyset$ and $R(\delta, \alpha_\delta^+, b) \neq \emptyset$. Therefore we have proved that $R(\delta, \alpha_\delta^+, v) \neq \emptyset$ and $R(\delta, \alpha_\delta^+ + \delta, u) \neq \emptyset$ for every $u, v \in GF(p^t)$. Due to the same reasoning, we have $\#(R(\delta, \alpha_\delta^+ + \delta, u) \cap R(\delta, \alpha_\delta^+, v)) = p^{-t} \#R(\delta, \alpha_\delta^+ + \delta, u)$ and $\#(R(\delta, \alpha_\delta^+, v) \cap R(\delta, \alpha_\delta^+ + \delta, u)) = p^{-t} \#R(\delta, \alpha_\delta^+, v)$ for every $u, v \in$

$GF(p^t)$. Comparing the above two equalities, we conclude that $\#R(\delta, \alpha_\delta^+ + \delta, u) = \#R(\delta, \alpha_\delta^+, v)$ for every $u, v \in GF(p^t)$. Therefore both $\#R(\delta, \alpha_\delta^+ + \delta, u)$ and $\#R(\delta, \alpha_\delta^+, v)$ are constant. Note that $\sum_{v \in GF(p^t)} \#R(\delta, \alpha_\delta^+, v) = p^{t(n-l)}$. We have proved that $\#R(\delta, \alpha_\delta^+, v) = p^{t(n-l-1)}$ for any $v \in GF(p^t)$. Thus we have proved that $\#(R(\delta, \alpha_\delta^+ + \delta, u) \cap R(\delta, \alpha_\delta^+, v)) = p^{t(n-l-2)}$ for every $u, v \in GF(p^t)$. For any $\tau \preceq \delta$, choose $\alpha \in GF(p^t)^n$ such that $\alpha_\delta^+ = \tau$. Clearly both conditions (i) and (ii) hold. Conversely assume the defining function f satisfies conditions (i) and (ii). Choose any $\delta \in GF(p^t)^n$ with $HW(\delta) = l$, where $1 \leq l \leq k$, as a cheating vector and any α as an original vector. Set $f(\alpha) = K$ and $f(\alpha + \delta) = K^*$. By definition, $\rho_{\delta,\alpha} = \#(R(\delta, \alpha_\delta^+ + \delta, K^*) \cap R(\delta, \alpha_\delta^+, K))/\#R(\delta, \alpha_\delta^+ + \delta, K^*)$. Due to conditions (i) and (ii), $\rho_{\delta,\alpha} = p^{-t}$. Thus we have proved that the secret sharing is k-cheating immune. □

Theorem 3. *Given a secret sharing with its defining function f on $GF(p^t)^n$. Then the following statements are equivalent: (i) this secret sharing is k-cheating immune, (ii) for any integer l with $1 \leq l \leq k$, any $\delta \in GF(p^t)^n$ with $HW(\delta) = l$, any $\tau \preceq \delta$ and any $u, v \in GF(p^t)$, we have $\#(R(\delta, \tau, v) \cap R(\delta, \tau + \delta, u)) = p^{t(n-l-2)}$, (iii) for such l, δ, τ, u and v mentioned in (ii), the system of equations:* $\begin{cases} f(x_\delta^- + \tau + \delta) = u \\ f(x_\delta^- + \tau) = v \end{cases}$ *has precisely $p^{t(n-l-2)}$ solutions on x_δ^-.*

Proof. Clearly (ii) $\Longleftrightarrow$ (iii). Due to Theorem 2, (i) $\Longrightarrow$ (ii). To complete the proof, we only need prove that (ii) $\Longrightarrow$ (i). Assume that (ii) holds. Thus $\#(R(\delta, \tau, v) \cap R(\delta, \tau + \delta, u)) = p^{t(n-l-2)}$ for every $u, v \in GF(p^t)$. Note that $R(\delta,\tau,v) = \cup_{u \in GF(p^t)} R(\delta, \tau, v) \cap R(\delta, \tau + \delta, u)$ and then $\#R(\delta, \tau, v) = \sum_{u \in GF(p^t)} \#(R(\delta, \tau, v) \cap R(\delta, \tau + \delta, u))$. This proves that $\#R(\delta, \tau, v) = p^{t(n-l-1)}$. Using Theorem 2, we have proved that (i) holds. □

2.2 Constructions of k-cheating Immune Secret Sharing

Let h is a function of degree two on $GF(p^t)^n$ and $\delta = \{\delta_1, \ldots, \delta_n)$ be a nonzero vector in $GF(p^t)^n$. Set $J = \{j \mid \delta_j \neq 0, \ 1 \leq j \leq n\}$. Let τ be any vector in $GF(p^t)^n$ with $\tau \preceq \delta$. It is easy to verify that $x_j x_i$ is a term in $h(x_\delta^+ + \tau) \Longleftrightarrow x_j x_i$ is a term in h also $j, i \notin J \Longleftrightarrow x_j x_i$ is a term in $h(x_\delta^+ + \tau + \delta)$. Thus $h(x_\delta^+ + \tau)$ and $h(x_\delta^+ + \tau + \delta)$ have the same quadratic terms, and thus $h(x_\delta^+ + \tau + \delta) - h(x_\delta^+ + \tau)$ must be an affine function. The function h of degree two is said to have the *property B(k)* if for any $\delta \in GF(p^t)^n$ with $1 \leq HW(\delta) \leq k$ and any $\tau \preceq \delta$, $h(x_\delta^+ + \tau + \delta) - h(x_\delta^+ + \tau)$ is a non-constant affine function.

Lemma 2. *Let f_1 and f_2 be two functions on $GF(p^t)^{n_1}$ and $GF(p^t)^{n_2}$ respectively. Set $f(x) = f_1(y) + f_2(z)$ where $x = (y, z)$ where $y \in GF(p^t)^{n_1}$ and $z \in GF(p^t)^{n_2}$. Then f is balanced if f_1 or f_2 is balanced,*

The above lemma can be verified directly. The special case of $p = 2$ and $t = 1$ was given in Lemma 12 of [8]. Using Lemma 2, we can prove

Lemma 3. *Let f_1 and f_2 be two functions of degree two on $GF(p^t)^{n_1}$ and $GF(p^t)^{n_2}$ respectively. Set $f(x) = f_1(y) + f_2(z)$ where $x = (y, z)$ where $y \in GF(p^t)^{n_1}$ and $z \in GF(p^t)^{n_2}$. Then f has the property B(k) if both f_1 and f_2 have the property B(k).*

Theorem 4. *Let k and s be two positive integers with $s \geq k+1$, h_j be a balanced function of degree two on $GF(p^t)^{n_j}$ satisfying the property B(k), $j = 1, \ldots, s$. Set $n = n_1 + \cdots + n_s$. Define a function f on $GF(p^t)^n$ such as $f(x) = h_1(y) + \cdots + h_s(z)$ where $x = (y, \ldots, z)$, h_i and h_j have disjoint variables if $i \neq j$. Then the secret sharing with the defining function f is k-cheating immune.*

Proof. Let $\delta = (\delta_1, \ldots, \delta_n) \in GF(p^t)^n$ with $HW(\delta) = l$, where $1 \leq l \leq k$. Let τ be any vector in $GF(p^t)^n$ with $\tau \preceq \delta$. Consider the system of equations: $\begin{cases} f(x_\delta^- + \tau + \delta) = u \\ f(x_\delta^- + \tau) = v \end{cases}$. Set $J = \{j \mid \delta_j \neq 0, \ \ 1 \leq j \leq n\}$. Note that $\#J = HW(\delta) = l$. We write $J = \{j_1, \ldots, j_l\}$. Since $l \leq k \leq s-1$, there exists some j_0 with $1 \leq j_0 \leq s$ such that each variable of h_{j_0} is not in $\{x_{j_1}, \ldots, x_{j_l}\}$. For the sake of convenience, we assume that $j_0 = s$ and thus h_s remains in both equations above. Thus if $j \in J$ then $j \leq n - n_s$. Write $x = (\mu, z)$, where $\mu \in GF(p^t)^{n-n_s}$ and $z \in GF(p^t)^{n_s}$. Define a vector $\sigma \in GF(p^t)^{n-n_s}$ such that $\sigma = (\sigma_1, \ldots, \sigma_{n-n_s})$ satisfying $\sigma_j = \delta_j$, $j = 1, \ldots, n - n_s$. Thus $HW(\sigma) = HW(\delta) = \#J = l$ and $x_\delta^- = (\mu_\sigma^-, z)$. We rewrite the above system of equations as $\begin{cases} g_1(\mu_\delta^-) + h_s(z) = u \\ g_2(\mu_\delta^-) + h_s(z) = v \end{cases}$ where both g_1 and g_2 are functions on $GF(p^t)^{n-n_s}$. Note that $x_j x_i$ is a term in $g_1 + h_s \iff x_j x_i$ is a term in f and $j, i \notin J \iff x_j x_i$ is a term in $g_2 + h_s$. Thus $g_1 + h_s$ and $g_2 + h_s$ have the same quadratic terms. Therefore $g_1 - g_2$ is an affine function. Set $g_2 - g_1 = \psi$. Note that the above system of equations is equivalent to $\begin{cases} g_1(\mu_\sigma^-) + h_s(z) = u \\ \psi(\mu_\sigma^-) = u - v \end{cases}$. Since each h_j has the property B(k), ψ is a non-constant affine function and thus the equation $\psi(\mu_\sigma^-) = u - v$ has $p^{t(n-n_s-l-1)}$ solutions on μ_σ^-. For each fixed solution μ_σ^- of the equation $\psi(\mu_\sigma^-) = u - v$, since h_s is balanced, $g_1(\mu_\sigma^-) + h_s(z)$ takes u precisely $p^{t(n_s-1)}$ times while z runs through $GF(p^t)^s$ once. Therefore the above system of equations has precisely $p^{t(n-n_s-l-1)} \cdot p^{t(n_s-1)} = p^{t(n-l-2)}$ solutions on $(\mu_\sigma^-, z) = x_\delta^-$. Due to Theorem 3, we have proved that the secret sharing with the defining function f, defined in the theorem, is k-cheating immune. □

Lemma 4. *Define a function χ_{2k+1} on $GF(p^t)^{2k+1}$ by $\chi_{2k+1}(x_1, \ldots, x_{2k+1}) = x_1x_2 + x_2x_3 + \cdots + x_{2k}x_{2k+1} + x_{2k+1}x_1$. Then (i) the function χ_{2k+1} is balanced, (ii) χ_{2k+1} satisfies the property B(k).*

Proof. By a nonsingular linear transform on the variables, the function χ_{2k+1} can be transformed to the form of $y_1y_2 + y_2y_3 + \cdots + y_{2k-1}y_{2k} \pm y_{2k+1}^2$. It is easy to verify that the function $h(y_1, \ldots, y_{2k+1}) = y_{2k+1}^2$ is balanced. Due to Lemma 2, χ_{2k+1} is balanced. Next we prove the part (ii) of the lemma. Let $\delta \in GF(p^t)^{2k+1}$ with $HW(\delta) = l$, where $1 \leq l \leq k$, and $\tau \preceq \delta$. Write $\delta = (\delta_1, \ldots, \delta_{2k+1})$ and $J = \{j \mid \delta_j \neq 0, \ \ 1 \leq j \leq 2k+1\}$. Clearly, $\#J = HW(\delta) = l$. The index $i \notin J$ is said to be *associated* with $j \in J$ if $x_j x_i$ is a term in χ_{2k+1}. Due to the structure of χ_{2k+1}, each $i \notin J$ is associated at most two elements of J. Since $l \leq k$, it is easy to verify that there exists some j_0 such that $j_0 \in J$, $j_0 + 1 \notin J$ and $j_0 + 1$ is associated with j_0 only – Case 1, otherwise there exists some j_0 such that $i_0 \in J$, $i_0 - 1 \notin J$ and $i_0 - 1$ is associated with i_0 only – Case 2. Assume Case 1 occurs. Write $\tau = (\tau_1, \ldots, \tau_{2k+1})$. Since $j_0 \in J$, we know that $\delta_{j_0} \neq 0$. Therefore $\delta_{j_0} x_{j_0+1}$ must appear in $\chi_{2k+1}(x_\delta^+ + \tau + \delta) - \chi_{2k+1}(x_\delta^+ + \tau)$. This proves that χ_{2k+1} has the property B(k) in Case 1. Similarly we can prove that χ_{2k+1} has the property B(k) in Case 2. □

Using Lemmas 2, 3 and 4, we obtain the following:

Lemma 5. *Define a function* χ_{4k+2} *on* $GF(p^t)^{4k+2}$ *by* $\chi_{4k+2}(x_1, \ldots, x_{4k+2}) = \chi_{2k+1}(x_1, \ldots, x_{2k+1}) + \chi_{2k+1}(x_{2k+2}, \ldots, x_{4k+2})$. *Then (i) the function* χ_{4k+2} *is balanced, (ii)* χ_{4k+2} *satisfies the property B(k).*

χ_n in Lemma 4 or 5 has been defined for odd n and even n with $n \equiv 2 \bmod 4$. Due to Lemma 4, Lemma 5 and Theorem 4, we have the following construction.

Theorem 5. *Let* k *and* s *be positive integers with* $s \geq k + 1$. *Let* $n_1, \ldots, n_s = 4k + 1$ *or* $4k + 2$, *and* $n = n_1 + \cdots + n_s$. *Define a function on* $GF(p^t)^n$ *such as* $f(x) = \chi_{n_1}(y) + \cdots + \chi_{n_s}(z)$ *where* $x = (y, \ldots, z)$, $y \in GF(p^t)^{n_1}, \ldots, z \in GF(p^t)^{n_s}$, *each* χ_{n_j} *has been defined in (4) or (5), and* $\chi_{n_1}, \ldots, \chi_{n_s}$ *have disjoint variables mutually. Then the secret sharing with the defining function* f *is* k*-cheating immune.*

Note that $n = n_1 + \cdots + n_s$, defined in Theorem 5, can be expressed as $n = (4k + 1)r + (4k + 2)q$ where $r \geq 0$ and $q \geq 0$ are integers. Since $4k + 1$ and $4k+2$ are relatively prime, any integer can also be written as $(4k+1)r+(4k+2)q$ where r and q are integers. Furthermore it is easy to verify that any integer n with $n \geq (4k + 1)^2$ can be expressed as $n = (4k + 1)r + (4k + 2)q$ where $r, q \geq 0$. Since $n \geq (4k + 1)^2$, $s = r + q > k + 1$ where s was mentioned in Theorem 5. Using Theorem 5, we can construct k-cheating immune secret sharing with n participants where $n \geq (4k + 1)^2$.

3 Generalised Model of Cheating

Given a function f on $GF(p^t)^n$, we introduce the following notations:

- Let $\alpha \in GF(p^t)^n$ be the sequence of shares held by the group $\mathcal{P} = \{P_1, \ldots, P_n\}$ of n participants and the secret $K = f(\alpha)$.
- The collection of cheaters is determined by the sequence $\delta = (\delta_1, \delta_2, \ldots, \delta_n)$ where P_i is a cheater $\Longleftrightarrow$ if $\delta_i \neq 0$.
- At the pooling time, the cheaters submit their shares. This time it is assumed that cheaters may submit a mixture of valid and invalid shares. The honest participants always submit their valid shares. The collection of cheaters who submit invalid shares is determined by the sequence $\tau = (\tau_1, \ldots, \tau_n)$ where $\tau_j = 0 \Longleftrightarrow P_j$ is honest or P_j is a cheater who submits a valid share, in other words, $\tau_j \neq 0 \Longleftrightarrow P_j$ is a cheater who submits an invalid share.

Clearly $\tau \preceq \delta$. We assume that there exists at least one cheater who submits invalid share, in other words, we only consider the case that τ is nonzero or $HW(\tau) > 0$. We consider the vector $\alpha + \tau$. Due to the properties of operations x_δ^+ and x_δ^-, $\alpha + \tau = \alpha_\delta^- + \alpha_\delta^+ + \tau$. The combiner obtains $\alpha + \tau$ that splits into two parts: α_δ^- – the part submitted by honest participants and $\alpha_\delta^+ + \tau$ the part submitted by cheaters. The combiner returns an invalid secret $K^* = f(\alpha + \tau)$.

- $R(\delta, \alpha_\delta^+ + \tau, K^*)$, or $\{x_\delta^- | f(x_\delta^- + \alpha_\delta^+ + \tau) = K^*\}$, where α_δ^+ determines valid shares held by the cheaters, represents the view of the cheater after getting back K^* from the combiner.
- The set $R(\delta, \alpha_\delta^+, K)$, or $\{x_\delta^- | f(x_\delta^- + \alpha_\delta^+) = K\}$, determines a collection of rows of $\mathcal{T}$ with the correct secret K and valid shares held by the cheaters.

In generalised model of cheating, τ is used to determine how to cheat while δ is only used to determine which participants are dishonest, therefore we can define δ as a $(0,1)$-vector in $GF(p^t)^n$. However, in basic model of cheating, δ is not only used to determine which participants are dishonest but also used to determine how to cheat, thus δ has a more general form.

The function f is called the *defining function*. The nonzero vector $\delta = (\delta_1, \ldots, \delta_n)$ is called a *cheating vector*, the nonzero vector $\tau \preceq \delta$ is called an *active cheating vector*, α is called a *original vector*. The value of $\rho_{\delta,\tau,\alpha} = \#(R(\delta, \alpha_\delta^+ + \tau, K^*) \cap R(\delta, \alpha_\delta^+, K)) / \# R(\delta, \alpha_\delta^+ + \tau, K^*)$ expresses the probability of cheater success with respect to δ, τ and α. As an original vector α is always in $R(\delta, \alpha_\delta^+ + \tau, K^*) \cap R(\delta, \alpha_\delta^+, K)$, the probability of successful cheating always satisfies $\rho_{\delta,\tau,\alpha} > 0$. Clearly the number of cheaters is equal to $HW(\delta)$ and the number of active cheaters is equal to $HW(\tau)$. In particular, if $\tau = \delta$, we regain basic model of cheating. From now, we consider secret sharing against cheating by generalised model of cheating.

3.1 Strictly k-cheating Immune Secret Sharing Scheme

By using the same arguments as in the proof of Theorem 1, we can state.

Theorem 6. *Given a secret sharing with its defining function f on $GF(p^t)^n$. Let $\delta \in GF(p^t)^n$ with $0 < HW(\delta) < n$ be a cheating vector, $\tau \preceq \delta$ with $\tau \neq 0$ be an active cheating vector, and $\alpha \in GF(p^t)^n$ be an original vector. If $\rho_{\delta,\tau,\alpha} < p^{-t}$ then there exists a vector $\gamma \in GF(p^t)^n$ such that $\rho_{\delta,\tau,\gamma} > p^{-t}$.*

For the same reason mentioned in Section 2.1, we introduce the concept of k-cheating immune secret sharing scheme. Given a secret sharing with its defining function f on $GF(p^t)^n$. Let k be an integer with $1 \le k \le n-1$. The secret sharing is said to be *strictly k-cheating immune* if the probability of successful cheating satisfies $\rho_{\delta,\tau,\alpha} = p^{-t}$ for every $\delta \in GF(p^t)^n$ and any $\tau \preceq \delta$ with $1 \le HW(\tau) \le HW(\delta) \le k$ and every $\alpha \in GF(p^t)^n$. The following is a relationship between the two models of cheating immune secret sharing.

Theorem 7. *Given a secret sharing with its defining function f on $GF(p^t)^n$. Then the secret sharing is strictly k-cheating immune $\Longleftrightarrow$ for any integer r with*

$0 \le r \le k-1$, any subset $\{j_1,\dots,j_r\}$ of $\{1,\dots,n\}$ and any $a_1,\dots,a_r \in GF(p^t)$, $f(x_1,\dots,x_n)|_{x_{j_1}=a_1,\dots,x_{j_r}=a_r}$, as a function on $GF(p^t)^{n-r}$ with the variables $x_{i_1},\dots,x_{i_{n-r}}$, where $\{i_1,\dots,i_{n-r}\} \cup \{j_1,\dots,j_r\} = \{1,\dots,n\}$, is the defining function on $GF(p^t)^{n-r}$ of a $(k-r)$-cheating immune secret sharing.

Proof. Assume that the secret sharing is strictly k-cheating immune. Let g be a function on $GF(p^t)^{n-r}$ given by $g = f(x_1,\dots,x_n)|_{x_{j_r}=a_1,\dots,x_{j_r}=a_r}$. Comparing basic model of cheating with generalised model of cheating, since f is the defining function on $GF(p^t)^n$ of a strictly k-cheating immune secret sharing in generalised model of cheating, we know that g is the defining function on $GF(p^t)^{n-r}$ of a $(k-r)$-cheating immune secret sharing against basic model of cheating. We have proved the necessity. By definition, we can invert the above reasoning and prove the sufficiency. □

3.2 Construction of Strictly k-cheating Immune Secret Sharing

Lemma 6. *Let a function f of degree two on $GF(p^t)^n$ do not have a nonzero constant term, in other words, $f(0,\dots,0) = 0$, where 0 denotes the zero element in $GF(p^t)$. Then f is balanced $\Longleftrightarrow$ there exists a nonzero vector $\alpha \in GF(p^t)^n$ such that $f(x+\alpha) - f(x)$ is constant and $f(\alpha) \ne 0$.*

Lemma 6 with $p = 2$ and $t = 1$ is a special case of the lemma in [4]. Lemma 6 can be proved using the same arguments as those used for the proof of the lemma in [4].

Lemma 7. *Let $\lambda_{n,p}$ be a function on $GF(p^t)^n$ ($n \ge 2p^2 + p$) defined by $\lambda_{n,p}(x_1,\dots,x_n) = x_1 + \sum_{j=1}^{n}(x_j x_{[j+1]_{(n)}} + x_j x_{[j+2]_{(n)}} + \cdots + x_j x_{[j+p]_{(n)}})$ where $[i]_{(n)}$ denotes the integer j such that $1 \le j \le n$ and $j \equiv i \bmod n$ (we replace i by $[i]_{(n)}$ as i is possibly greater than n). Then (i) $\lambda_{n,p}$ is balanced, (ii) for any r with $0 \le r \le p-1$, any subset $\{j_1,\dots,j_r\}$ of $\{1,\dots,n\}$ and any $a_1,\dots,a_r \in GF(p^t)$, $\lambda_{n,p}(x_1,\dots,x_n)|_{x_{j_1}=a_1,\dots,x_{j_r}=a_r}$, as a function on $GF(p^t)^{n-r}$ with the variables $x_{i_1},\dots,x_{i_{n-r}}$, where $\{i_1,\dots,i_{n-r}\} \cup \{j_1,\dots,j_r\} = \{1,\dots,n\}$, satisfies the property B(p).*

Proof. From the construction of $\lambda_{n,p}$, for any j with $1 \le j \le n$, there precisely exist $2p$ quadratic terms of $\lambda_{n,p}$: $x_j x_{[j+i]_{(n)}}$ and $x_j x_{[j-i]_{(n)}}$ containing x_j where $i = 1,\dots,p$. It is easy to verify that $\lambda_{n,p}$ has precisely np quadratic terms, in addition, a linear term x_1. Set $g = \lambda_{n,p} - x_1$ or $g(x_1,\dots,x_n) = \sum_{j=1}^{n}(x_j x_{[j+1]_{(n)}} + x_j x_{[j+2]_{(n)}} + \cdots + x_j x_{[j+p]_{(n)}})$, and $\alpha = (1,\dots,1)$ where 1 denotes the identity in $GF(p^t)$. Recall that the characteristic of the finite field $GF(p^t)$ is p. Then $pe = 0$ holds for any element $e \in GF(p^t)$. Thus it is easy to verify that $g(x+\alpha) - g(x) = 0$ and $g(\alpha) = 0$. Therefore $\lambda_{n,p}(x+\alpha) - \lambda_{n,p}(x) = 1$ and $\lambda_{n,p}(\alpha) = 1$. Due to Lemma 6, we know that $\lambda_{n,p}$ is balanced. Next we prove the part (ii) of the lemma. Write $h(x_{i_1},\dots,x_{i_{n-r}}) = \lambda_{n,p}(x_1, \dots, x_n)|_{x_{j_1}=a_1,\dots,x_{j_r}=a_r}$. Set $x_{i_1} = y_1,\dots,x_{i_{n-r}} = y_{n-r}$ and $y = (y_1,\dots,y_{n-r})$. Then we consider the function $h(y_1,\dots,y_{n-r})$. Recall that for each j, $1 \le j \le n$, x_j appears precisely in $2p$ quadratic terms of $\lambda_{n,p}$: $x_j x_{[j+i]_{(n)}}$ and $x_j x_{[j-i]_{(n)}}$ where $i = 1,\dots,p$. Since

$r \leq p-1$, it is easy to see that for each j, $1 \leq j \leq n-r$, there at least two quadratic terms of h. Let $\delta \in GF(p^t)^{n-r}$ be a cheating vector with $HW(\delta)=l$, where $1 \leq l \leq p$, and $\tau \preceq \delta$ be an active cheating vector. Write $\delta=(\delta_1,\ldots,\delta_{n-r})$ and $J=\{j \mid \delta_j \neq 0,\ 1 \leq j \leq n-r\}$. Clearly $\#J = HW(\delta)=l$. We do not need to consider any term $y_j y_i$ in h with $j,i \notin J$ as it does not appear in $h(y_\delta^+ + \tau + \delta) - h(y_\delta^+ + \tau)$. Since $n-r \geq 2p^2+1$, there exist some integers j_0 and m such that $m \geq 2p+1$, $[j_0+m]_{(n-r)} \in J$ and $\{[j_0+1]_{(n-r)}, [j_0+2]_{(n-r)}, \ldots, [j_0+m-1]_{(n-r)}\} \cap J = \emptyset$. Due to the structures of $\lambda_{n,p}$ and h, there exists some $[i_0]_{(n-r)} \in \{[j_0+1]_{(n-r)}, [j_0+2]_{(n-r)}, \ldots, [j_0+m-1]_{(n-r)}\}$ such that $y_{j_0} y_{[i_0]_{(n-r)}}$ is a term in h but $y_{[j_0+m]_{(n-r)}} y_{[i_0]_{(n-r)}}$ is not a term in h. Furthermore, due to the structures of $\lambda_{n,p}$ and h, $y_j y_{[i_0]_{(n-r)}}$ cannot be a term in h for any $j \in J$ with $j \neq j_0$. Since $[i_0]_{(n-r)} \notin J$, as the discussion before, any term $y_j y_{[i_0]_{(n-r)}}$ with $j \notin J$ does not appear in $h(y_\delta^+ + \tau + \delta) - h(y_\delta^+ + \tau)$. Since $j_0 \notin J$, we know that $\delta_{j_0} \neq 0$. Therefore $\delta_{j_0} y_{[i_0]_{(n-r)}}$ appears in $h(y_\delta^+ + \tau + \delta) - h(y_\delta^+ + \tau)$. This proves that h has the property B(p). □

Based on Theorem 7 and Lemma 7, we have the following construction.

Theorem 8. *Let $GF(p^t)$ be a finite field, s be an integer with $s \geq 2p$. Let $n_1, \ldots, n_s = 2p^2+p$ or $2p^2+p+1$, and $n = n_1 + \cdots + n_s$. Define a function on $GF(p^t)^n$ such as $f(x) = \lambda_{n_1,p}(y) + \cdots + \lambda_{n_s,p}(z)$ where $x=(y,\ldots,z)$, $y \in GF(p^t)^{n_1}, \ldots, z \in GF(p^t)^{n_s}$, each $\lambda_{n_j,p}$ has been defined in Lemma 7 and $\lambda_{n_i,p}, \ldots, \lambda_{n_j,p}$ have disjoint variables if $i \neq j$. Then the secret sharing with the defining function f is strictly p-cheating immune.*

Proof. Let r be an integer with $0 \leq r \leq p-1$ and $\{j_1, \ldots, j_r\}$ be a subset of $\{1, \ldots, n\}$. Since $r \leq p-1$, there exist at least $s-r \geq p+1$ functions among $\lambda_{n_1,p}, \ldots, \lambda_{n_s,p}$, each of whose variables is not included in $\{x_{j_1}, \ldots, x_{j_r}\}$. Without loss of generality, we assume that each variable of $\lambda_{n_{r+1},p}, \ldots, \lambda_{n_s,p}$ is not included in $\{x_{j_1}, \ldots, x_{j_r}\}$. Therefore for any $a_1, \ldots, a_r \in GF(p^t)$, f can be expressed as $f|_{x_{j_1}=a_1,\ldots,x_{j_r}=a_r} = g + \lambda_{n_{r+1},p} + \lambda_{n_{r+2},p} + \cdots + \lambda_{n_s,p}$ where $g = (\lambda_{n_1,p} + \cdots + \lambda_{n_r,p})|_{x_{j_1}=a_1,\ldots,x_{j_r}=a_r}$. Due to Lemmas 7,
$\lambda_{n_j,p}|_{x_{j_1}=a_1,\ldots,x_{j_r}=a_r}$ has the property B(p), $j=1,\ldots,r$ and thus from Lemma 3, g has the property B(p) and thus $f|_{x_{j_1}=a_1,\ldots,x_{j_r}=a_r}$ has the property B(p). Since each $\lambda_{n_j,p}$ is balanced, due to Lemma 2, $f|_{x_{j_1}=a_1,\ldots,x_{j_r}=a_r}$ is balanced. Applying Theorem 4 to $f|_{x_{j_1}=a_1,\ldots,x_{j_r}=a_r} = g + \lambda_{n_{r+1},p} + \lambda_{n_{r+2},p} + \cdots + \lambda_{n_s,p}$, we conclude the secret sharing with the defining function $f|_{x_{j_1}=a_1,\ldots,x_{j_r}=a_r}$ is p-cheating immune. Finally, using Theorem 7, we know that the secret sharing with the defining function f is strictly p-cheating immune. □

By using the same arguments as in the last paragraph of Section 2.2, it is easy to verify that any integer $n \geq (2p^2+p)^2$ can be expressed as $n = r(2p^2+p) + q(2p^2+p+1)$ where $r, q \geq 0$. Since $n \geq (2p^2+p)^2$, $s = r+q \geq 2p$ where s was mentioned in Theorem 7. Using Theorem 7, we can construct p-cheating immune secret sharing with n participants where $n \geq (2p^2+p)^2$.

4 Conclusions and Remarks

We have considered secret sharing over finite field and its resistance against cheating by a group of k dishonest participants. We have proved that the probability of successful cheating is always higher than p^{-t}. The secret scheme is said to be k-cheating immune if the probability of successful cheating is p^{-t} for any group of k or less participants. We have characterised k-cheating immune secret sharing scheme by examining its defining function. This characterisation enables us to construct k-cheating immune secret sharing scheme. Being more precise, we have studied two cases. In the first case, the group of cheaters always submit invalid shares. While in the second case, the group is more flexible as they collectively decide which of their shares should be modified and which should be submitted in their original form.

Acknowledgement

The first author was supported by the Large ARC Grant A00103078. The second author was supported by a Queen Elizabeth II Fellowship (227 23 1002).

References

1. M. Carpentieri. A perfect threshold secret sharing scheme to identify cheaters. *Designs, Codes and Cryptography*, 5(3):183–187, 1995.
2. M. Carpentieri, A. De Santis, and U. Vaccaro. Size of shares and probability of cheating in threshold schemes. *Advances in Cryptology - EUROCRYPT'93*, LNCS No. 765, pages 118–125. Springer-Verlag, 1993.
3. P. Feldman. A practical scheme for non-interactive verifiable secret sharing. In *Proceedings of the 28th IEEE Symposium on Foundations of Computer Science*, pages 427–437. IEEE, 1987.
4. K. Nyberg and L. R. Knudsen. Provable security against differential cryptanalysis. In *Advances in Cryptology - CRYPTO'92*, LNCS No. 740, pages 566–574. Springer-Verlag, 1993.
5. T.P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In J. Feigenbaum, editor, *Advances in Cryptology - CRYPTO'91*, LNCS No. 576, pages 129–140. Springer-Verlag , 1992.
6. T. Rabin and M. Ben-Or. Verifiable secret sharing and multiparty protocols with honest majority. In *Proceedings of 21st ACM Symposium on Theory of Computing*, pages 73–85, 1989.
7. B. Schoenmakers. A simple publicly verifiable secret sharing scheme and its application to electronic voting. In M. Wiener, editor, *Advances in Cryptology - CRYPTO'99*, LNCS No. 1666, pages 148–164. Springer - Verlag, 1999.
8. J. Seberry, X. M. Zhang, and Y. Zheng. Nonlinearity and propagation characteristics of balanced boolean functions. *Information and Computation*, 119(1):1–13, 1995.
9. M. Stadler. Publicly verifiable secret sharing. In U. Maurer, editor, *Advances in Cryptology - EUROCRYPT'96*, LNCS No. 1070, pages 190–199. Springer-Verlag, 1996.
10. D.R. Stinson. *Cryptography: Theory and Practice.* CRC Press, 1995.
11. Martin Tompa and Heather Woll. How to share a secret with cheaters. In A.M. Odlyzko, editor, *Advances in Cryptology - CRYPTO'86*, LNCS No. 263, pages 261–265. Springer-Verlag, 1987.